Critical Criminology

'Meum and Tuum'; cybercrime as the negative externality of 'post-politics bio-politics'

--Manuscript Draft--

Manuscript Number:	
Full Title:	'Meum and Tuum'; cybercrime as the negative externality of 'post-politics bio-politics'
Article Type:	Original Article
Keywords:	Cybercrime; Neoliberalism; Subjectivation; Capitalism; Debt
Corresponding Author:	Mwenda Wilson Kailemia, PhD Keele University Newcastle-Under-Lyme, UNITED KINGDOM
Corresponding Author Secondary Information:	
Corresponding Author's Institution:	Keele University
Corresponding Author's Secondary Institution:	
First Author:	Mwenda Wilson Kailemia, PhD
First Author Secondary Information:	
Order of Authors:	Mwenda Wilson Kailemia, PhD
Order of Authors Secondary Information:	
Funding Information:	
Abstract:	The purpose of this article is to offer a critical analysis of the 'violence of capitalism' (Lazzarato, 2014; Zizek, 2009; Kovel, 2007; Foster et al, 2010) apropos of cybercrime. Deploying recent examples of 'DIY Jihadi terrorism' (Conway, 2012; Awan and Al-Alami, 2009; Veilleux-lepage, 2016), 'School shooter fandoms' (Duffet, 2013; Daggett, 2015; Cullen, 2015; Curran, 2012; Hellekson and Busse, 2006) and 'Revenge porn' (Bates, 2015; Calvert, 2013; Citron and Franks, 2014) we show how these forms of cybercrime are 'externalized'-that is constituted as necessary costs of doing business-through the neoliberal methodology which Zizek (2014) apropos of Lazzarato (2011;14) has described as 'entrepreneurships-of-the-self'. The purpose of such entrepreneurship is to 'privatize the social and socialize the private'; that is to dichotomize subjects of capitalism into those who owe and those who are owed, through a new moral order of indebtedness (guilt, fear, shame, revenge and so forth) (Zizek, 2014; Lazzarato, 2011; 2014).

TITLE PAGE

Name:	Dr. Mwenda Kailemia
Address	Mwenda W Kailemia School of social Science and Public Policy Keele University Keele, Staffs ST55BG.
Contact details	Email: m.l.w.kailemia@keele.ac.uk Tel: 0178234166

Title	***''Meum and Tuum'; cybercrime and the negative externality of 'post-politics bio-politics'***
Autobiographical note	Mwenda Kailemia is a lecturer in Criminology in the school of Social Science and Public Policy, Keele University. His main areas of research interest are: Neoliberalism and the violence of Capital, especially as it relates to Race and ethnic diversity, transnational crimes, crimes against humanity and environmental crimes.
Key words	Cybercrime; Capital; Post-politics bio-politics; externality; Ecological Disorganization; Subjectivity; Neoliberalism; Debt;

Abstract

Abstract

The purpose of this article is to offer further analysis of the 'violence of capitalism' (Lazzarato, 2014; Zizek, 2009; Kovel, 2007; Foster et al, 2010). Deploying recent analyses of cybercrime, and specifically 'DIY Jihadi terrorism' (Conway, 2012; Awan and Al-Alami, 2009; Veilleux-lepage, 2016), 'School shooter fandoms' (Duffet, 2013; Daggett, 2015; Cullen, 2015; Curran, 2012; Hellekson and Busse, 2006) and 'Revenge porn' (Bates, 2015; Calvert, 2013; Citron and Franks, 2014) we show how these forms of cybercrime are 'externalized'-that is constituted as necessary costs of doing business- through the neoliberal methodology which Zizek (2014) apropos of Lazzarato (2011;14) has described as 'entrepreneurships-of-the-self'. The purpose of such entrepreneurship is to 'privatize the social and socialize the private'; that is to dichotomize subjects of capitalism into those who owe and those who are owed, through a new moral order of indebtedness (guilt, fear, shame, revenge and so forth) (Zizek, 2014; Lazzarato, 2011; 2014)

'Meum and Tuum'; cybercrime as the negative externality of post-politics bio-politics

Abstract

The purpose of this article is to offer a critical analysis of the 'violence of capitalism' (Lazzarato, 2014; Zizek, 2009; Kovel, 2007; Foster et al, 2010) apropos of cybercrime. Deploying recent examples of 'DIY Jihadi terrorism' (Conway, 2012; Awan and Al-Alami, 2009; Veilleux-lepage, 2016), 'School shooter fandoms' (Duffet, 2013; Daggett, 2015; Cullen, 2015; Curran, 2012; Hellekson and Busse, 2006) and 'Revenge porn' (Bates, 2015; Calvert, 2013; Citron and Franks, 2014) we show how these forms of cybercrime are 'externalized'-that is constituted as necessary costs of doing business- through the neoliberal methodology which Zizek (2014) apropos of Lazzarato (2011;14) has described as 'entrepreneurships-of-the-self'. The purpose of such entrepreneurship is to 'privatize the social and socialize the private'; that is to dichotomize subjects of capitalism into those who owe and those who are owed, through a new moral order of indebtedness (guilt, fear, shame, revenge and so forth) (Zizek, 2014; Lazzarato, 2011; 2014).

Introduction: 'Externality and capitalism's 'necessity of harm'

Hayek (1973:101), invoking the economists' *lingua,* introduced the concept of 'externalities' to refer to the logic of business in which actions that are not manifestly intended to cause harm to others cannot become the subject of rules of conduct. Apropos of 'externality', Hayek argued that 'some harm knowingly caused to others is even essential for the preservation of spontaneous order' (1973: 1101) so that, to take one example, the state, exercising its prerogatives through the law, is only interested in harms if they destabilise the (spontaneous order of the) system as a whole (and not necessarily because they are harms as such) (see also Ruggierro, 2013; Ruggierro and South, 2013). The law, for example, cannot prohibit 'the setting up of a new business even if this will lead to the failure of another', as Hayek (1973: 102) observed- or, to stretch the logic further, the state cannot intervene unless there is a clear case that systematic dysfunction threatens not only the whole of other systems, but the relationships of such systems to the state. In this articulation, law and legality incorporate a range of conflicting expectations so that the prerogative of the state- or a system of states- is to decide which one prevails.

In theory, this 'experimental' approach to the impact of business practices is unproblematic; it is not (always) possible or desirable, after all, to prevent all actions which are likely to harm some, while benefitting others (Hayek, 1973; Ruggierro, 2013). In practice, however, justification for the necessity or desirability of harm is usually accompanied by a view of the entitlement of the 'other'(s) as a subject of constant review and change (Zizek, 2014; Lazzarato, 2014; Ruggierro and South, 2013). Hayek was already aware of this when, in his conceptualization of externalization as 'the establishment of the precise boundaries within which action is acceptable', he also cautions that 'externalization' can also mean 'the demarcation of a range of objects over which only particular individuals are allowed to dispose and from the control of which all others are excluded' (Hayek 1973: 107). To put it in familiar terms, while democratized access to certain risky things may be justified by the prospect of collective gain, this alone cannot be enough to occlude assessment of how, in effect, such harms are distributed: Recent research on the harms of globalized capital (for example, Lazzarato, 2014; Zizek, 2014; Stiglitz, 2012) has for example outlined the differential and differentiating 'price of inequality' (from the collapse of the global ecosystem, to the threat of new species of diseases to the spread of psychosocial and neurotic disorders related to inequality).

In this sense, violence is already staged in capitalism (Zizek, 2009; Lazzarato, 2011; South, 2013) not only on account of its proclivity to exclude (Kovel, 2007; Foster et al. 2010), but because such exclusion constitutes 'objective' violence (Zizek, 2009) which is not only systemic, but also 'normalized'. Capitalism, *in nuce*, is violent.

While this analysis is not new, it is the point of contact it has with the distinction Hayek (1973) draws between *meum* and *tuum* ('mine' and 'thine') that should exercise our attention: As Hayek observed, while the social boundary-making concepts of *meum* and *tuum* encapsulate the law's aim of merely preventing, as much as possible, the actions of different individuals from interfering with each other, such prevention may also function as the legitimating façade of social inequality. This is also Zizek's (2009) reading of 'objective' violence: *Mutatis Mutandis*, laws are seized of matters only in tandem with considerations of the equation of power (see also, Kovel, 2007; Foster et al. 2010), or, as Kovel (2007) points out, laws (and policy) constitute the refraction of power through the spectrum of socio-economic interests.

The design of *Meum and tuum* is thus that of 'insiders' and 'outsiders'; those who are owed and those who owe. Apropos of cybercrime, there are, on the one hand, those who are placed outside the protective ambit of social justice, such as victims of so-called revenge porn who are blamed for their carelessness (Stroud, 2014; Linkous, 2013; Calvert, 2013); or the victors of online commerce, such as corporate tax payers who not only benefit from the 'property' posted on their sites by users, but also have the attention of the state and are protected through immediate outputs including through policy legal changes, or privileged access to tax havens(Zizek, 2014)[1].

'Meum and Tuum' and the entrepreneur-of-the-self.

This logic of *meum and tuum* has recently been diagnosed by Lazzarato (2011) and Zizek (2014) as 'subjectivation', which involves the 'privatization of the social' and the 'socialization of the private' through the deployment of debt as a tool of government. The aim of (debt) subjectivation, Zizek claims, is the construction of the individual as an entrepreneur-of-the-self through her transformation from a worker/labourer, for example, to a form of 'personal capital'. This 'financialization' of citizenship (Lazzarato, 2011:23) means, for example, that one's patterns of public or private services consumption constitute 'investment decisions', with one's worth and desirability calculable alongside the echelons and prestige of spaces one inhabits. Here is Lazzarato:

> The dedication, subjective motivation, and *the work-on-the-self* preached by management since 1980s have become an injunction to *take upon oneself* the costs and risks of the economic and financial disaster. The population must take charge of everything that business and the Welfare State 'externalize' onto society, debt first of all. (2011:9).

What Lazzarato is implying above is that, as the individual emerges as 'capital'- and thus the subject of corporate manipulation- she is no longer viewed as a citizen (with state protection), but as a form of investment decisions (on the best anti-virus, the best web-hosting site, the riskiest places to post online content and so forth) (see also, Lazzarato, 2011). The implication of this shift from citizen to entrepreneur is thus that risks (financial,

[1] But there is also a reversal of this logic, with the state and its citizens as victims (of costs of cybercrime which are transferred to them through utility bills and policing costs) or the state as a victim when it cannot count on the compliance of corporations (such as when the state needs to access important information to police or prosecute crime organized or perpetrated online.

ecological, and psychological) are outsourced from the corporation and the state (from insurance, to online markets to banking institutions and so forth) to the individual: Social protections are individualized (privatized) to align them to market norms (you are hacked because you did not do something you should have and so forth), and thus they are no longer guaranteed, but are conditional on the performance of the individual whose life is opened up for assessment (was your software up to date? Did you switch your provider?).

At the end of this process, the individual emerges precarious, isolated and subject to 'governance' through fear (Zizek, 2012) has diagnosed as *post-politics bio-politics*[2]: The individual is blamed for his condition (unemployment, stress, bad credit, loss of privacy) but also encouraged to take personal responsibility, to show some guilt, to take some action, against the object of her fear (cybercrime, refugees, terrorists and other undesirables). As Lazzarato argues,

> The subjective achievements neoliberalism had promised (''everyone a shareholder, everyone an owner, everyone an entrepreneur'') have plunged us into existential condition of the indebted man, at once responsible and guilty for his particular fate' (2011:9)

To understand the import of the above, however, we must understand Lazzarato's conceptualization of 'indebtedness'. For Lazzarato, debt reaches beyond 'money owed', encompassing all aspects of subjectivation (such as the guilt of not meeting social expectations and so forth) which, as he argues, the machinery of state-corporate symbiosis exists to extract:

> Debt acts as a 'capture, and 'predation' and 'extraction' machine on the whole of society, as an instrument for macroeconomic prescription and management, and as a mechanism for income redistribution. It also functions as a mechanism for the production and 'government' of collective and individual subjectivities…Debt produces a specific morality…The morality of debt results in moralization of the

[2] Zizek (2014) defines '*post-political bio-politics'* as a type of politics (and economics) which claims to 'leave everything behind' (old ideological struggles, old injustices…) to achieve the primary goal of the efficient administration of life (pp. 34). The purpose of post-political bio-politics, Zizek argues, is objectification of social life, so that it can be administered through fear: Instead of radical emancipation, the political subject is encouraged to accept and move on (forget apartheid, forget the stolen money in offshore accounts; just create a conducive environment for investors; acquire new voting machines; arm yourself with the latest software…).

> unemployed, the 'assisted', the users of services, as well as entire populations…The media and politicians have only one message to communicate: 'You are at fault', You are guilty' (2011:42).

Let us see, below, how post-politics bio-politics extracts this debt apropos of cybercrime.

The cyberworld as post-politics bio-politics

In tandem with Zizek (2014) and Lazzarato (2011) it is possible to conceptualize the cyberworld as the new site of governance through the new morality of indebtedness: Victims of internet fraud are constructed, not as collective victims of the failure of online market infrastructure, but as gullible and/or greedy individuals who did not take the appropriate steps required of them (such as buying or updating their 'anti-virus', reporting their victimization on time and so forth) (see also, Calvert, 2013; Laird, 2013; Kowalski et al. 2012). Isn't contemporary emphasis on outputs (new laws, new legislations, new white papers…), as opposed to outcomes (such as the requirement for online service providers to notify and compensate victims of violence or fraud perpetrated on their infrastructure), an example of the 'privatization of the social and the socialization of the private'? Indeed: In the present time, the internet has become, not only a place where the capable (conniving individuals, but also corporations) prey on their victims (Stroud, 2014; Wall, 2007; Moore, Yar, 2013), but also a place where perpetrators have been given the equipment and free access to a pool of potential victims (Quarshie and Odoom, 2012; Yar, 2013; Wall, 2007)

Like other examples of externalized harms under so-called globalization (see, for example, Stiglitz, 2012; Aas, 2007; Gros, 2003), the harms of cybercriminality are experienced more in 'developing countries' (which, as a rule, have less technical know-how and resources to fight fraud but are under increasing pressure to open up their economies to global finance). As Quarshie and Odoom (2012) observe, it is difficult to assess, much less police, cybercrime in Africa, not only because of the weak framework of laws vis-à-vis the 'corporate veil' of multinational companies, but also because such corporations only allow cross-jurisdictional boundaries to be crossed where investigations are in line with their

interests[3]. Where the company has something to hide (say, in terms of the weakness of its infrastructure) it may either construct breaches on its system as an 'internal problem' for its investigators, or only allow proceedings to take place in the jurisdiction of 'applicable law' (cue expensive trials in Western courts under Western laws) (see also, Ruggiero and South, 2013). This expensive undertaking dissuades states form even considering taking on powerful corporations choosing, instead, to allow the corporations to self-police[4]. As such, Quarshie and Odoom (2012) tells us, cybercrime laws in Africa are[5] for example likely to be found at the bottom of the 'priority list' when governments are negotiating the terms of foreign direct investments[6].

The point not to be missed here is that, under the globalization of neoliberalism, cybercrime has emerged as the example *par excellence* of the externalized harms of capital, for example through the relocation of cybercriminals to jurisdictions/regions where the laws are lax or inadequate or where the investigatory capacity is moribund (see also, Aas, 2007; Gros, 2003). These places encapsulate Gros' (2003) 'trouble in paradise' hypothesis: They are defrauded of badly-need revenue, or become hot-beds of conflict, as the examples cyber-jihadi below show. They are also under-protected and under-compensated. The citizens of such 'wastelands of globalization' (Aas, 2007; Stiglitz, 2012) are on their own-neoliberal's failed entrepreneurs-of-the-self. To take an example, Africa, which now has the

[3] As a result, jurisdiction, extraterritorial evidence and international cooperation are added to the complex nature of fighting cybercrime. Yar (2013) argues that other issues of 'where to prosecute' and extradition might arise, as cybercrime may be recognized as a crime in one jurisdiction and not in the other.

[4] According to Wall (2007) although cybercrime affects a large number of victims, it is also a 'low impact crime'. For Africa, it means, for example, that law enforcement agencies are always reluctant to pursue cybercriminals because of the nominal sum involved, say in fraud, or because of a lack of resources that are rather utilised to deal with real world crime, and to tackle more pressing economic problems.

[5] Because most African countries do not have laws covering cybercrime, it makes it very difficult for law enforcement agencies to prosecute perpetrators for an act that has not been defined in the penal code as a crime. Only five countries (Cameroon, Kenya, Mauritius, South Africa and Zambia) out of fifty four on the continent have laws on cybercrime (Global Centre for ICT in Parliament, 2014), with Nigeria and Tanzania to soon join the fight.

[6] There are other issues in relation to policing cybercrime for such countries, of course: Cybercrimes are not easily picked up by law enforcement agencies because they have little experience in dealing with cybercrime and the limited resources at their disposal can act as an obstacle in tackling the issue (Bande, 2013); law enforcement agencies have difficulties carrying out proper investigations because of the 'no boundary' nature of the internet; police officers are more accustomed to traditional crime investigating trends such as routine and physical crime scenes (hence they are less productive vis-à-vis 'non-routine' crimes) and so forth.

longest list of 'failed states,[7]'is emerging as a new frontier of cybercrime[8]. Even then, in comparison to the spread of online-Jihad[9] in the middle-east, Africa is a 'walk in the park'. Let us see how, below.

The online externality of post-9/11 anti-terrorism

As recent critiques of terrorism have pointed out, the deployment IT techniques- for example the use of Twitter by the so-called 'Islamic State' (Friedland, 2014) - represents a turning point within global jihadist movements. There is, in the incorporation of cyber-techniques into the methodologies of terrorism, a clear shift away from the highly organization-centric model (advanced by al-Qaeda, for example) towards one where unaffiliated sympathizers can interact with and, to some extent, shape propaganda content in real-time by actively participating in its further dissemination. Thus, what was once the problem of ideological and politico-economic 'strains' (Agnew, 2010; Cottee, 2010) is now the new normal of the 'jousance' of postmodern consumerism, where violence is staged and visibly consumed (Kailemia, 2016; Zizek, 2014).

What happened? To what is this shift on account of? Veilleux-lepage (2016) has diagnosed it: The evolution of online Jihad occurred in tandem with the industry liberalization which was forced on large parts of the so-called 'developing countries' at the turn of the 21st century (see for example, Zizek, 2014; Moyo, 2009; Weimann, 2006). At that point the problems of terrorism were blamed on the technical backwardness of such places, with global multinationals pushing for liberalisation of key sectors such as banking, telecommunications and defence. As Weimann (2006) has also noted, the phase of 'modernization' at the turn of the century meant that control of vital industry had shifted from the central government (obligated to provide security, but also enhance/direct economic growth) onto global multinationals (local shareholders and those from rich countries) who, as is standard, prioritized growth of the market, whilst conveniently

[7] See for example, http://fsi.fundforpeace.org/

[8] South Africa, to take one example, has consistently been placed among the top three counties with the highest cybercrime victims in the world (with Russia and China in the lead- according to the US 'Norton report' (see also, CNBC AFRICA, 2013, online)

[9] There is no consensus on what this term exactly means, or within which parameters it should be deployed. In our conceptualization, it merely denotes someone- or the idea of- violent Islam, also called Islamism. The intent is to refer to the idea or person who carries out or promotes violence as a methodology of converting to or punishing non-adherence to the ideology of fundamentalist Islam.

abstaining from the 'dark side' of such market. In this sense, whilst the jihadist presence in cyberspace remained limited until early 2000s, the rudimentary platforms which sprang up after the market liberalizations laid the groundwork for the ascendancy of more sophisticated and interactive uses of the Internet in this century. The 2000s were for example characterized by the explosion of interactive content (and the connected user participation) in the form of Web 2.0 online forums (Weimann, 2006). At this point, users not only consumed online content but also actively contributed to its creation (Warren and Leitch, 2012; Hoeren and Vossen, 2009), translating to glorious profits for platforms such as Facebook, which followed shortly. As the profits and popularity of such forums increased, the role and power of the state decreased concomitant with the clout the corporations invoked (to the extent it suited them) on privacy and intellectual property rights; that is to say, the issue of privacy and rights predominated, not because such forums were *ab initio* champions of privacy and rights- after all, most of these companies underpay their workers and in any case make profits out of the property (such as videos and photos) of their owners (Zizek, 2014; Lazzarato, 2011- but because, in invoking the notion of rights, these corporations could get the backing of their powerful home states.

Although matters were complicated by the dismal human rights record of the new frontiers of capital, the issues of rights were coincidental to the bigger logic of gaining and security an important market. As Zizek (2014) and Chomsky (2014) also acknowledge, the 'glocalization' of capital allowed the ostensible emergence of 'rights champions' among the ranks of multinational internet companies, clearly rendering the logic of capitalist externalization: In order to secure their market base, such corporations staged an 'online coup' on such states, offering the space to ventilate or create which was hitherto occluded (but not extending the same space for a challenge on their market monopoly or their appropriation of the intellectual property of their users).

The explosion in globalization of 'online forums' also coincided with the 2001 9/11 attacks: The post-9/11 period, Awan and Al-Alami (2009) and Veilleux-lepage (2016) show, was marked by a 'shifting security paradigm', with various groups of counter-terrorism hackers engaged in complex campaigns to disrupt jihadist websites. But, this only dislocated the online activity of jihadists, who began to decentralize their activity, for example from jihadist websites, which governments took down, to online forums (Awan and Al-Lami,

2009:57-58)[10]. This shift in paradigm is best embodied by the media strategy of Al Qaeda's (AQ) Abu Musab al-Zarqawi, and lately, by the so-called Islam State (IS): In early 2004, al-Zarqawi, utilizing the shift from Web 1.0 to the fully-fledged Web 2.0. (Conway, 2012), issued a video explaining who he was, why he was fighting, and providing details of the attacks he and his groups were responsible for.[11] Subsequently, capitalizing on this newfound recognition, Al Qaeda in Iraq (AQI) released a video titled *Abu Musa'b al-Zarqawi slaughters an American,* which depicted the beheading of the American civilian contractor Nicholas Berg (Conway, 2012). This video was uploaded to ogrish.com, a popular shock site, and was – as a result– viewed over 15 million times (Talbot, 2005). As others (for example, Maggioni, 2015) have pointed out, the video of Nick Berg's beheading marked a significant change in jihadist propaganda, into the present standard script: Westerners kneeling down with Kalashnikov-armed [jihadists] standing behind them, beg the governments of the west to reconsider their foreign policy initiatives, such the invasion of Muslim countries or the release of Jihadis in jails and so forth.

The point here is that, jihadist groups (operating in Iraq and elsewhere) seized on the power of easy-to-access video-sharing technology (and websites such as YouTube), but also the ubiquitous (but, deliberately hard to regulate) structures of online global commerce: Aided by the popularity of new media (and the fact that no Arabic language skills or high level of Internet literacy were now required to locate jihadist content), platforms such as YouTube rapidly became a significant platform for jihadist groups and their supporters, fostering a thriving subculture which they utilized for the dissemination of propaganda (see also, Veilleux-lepage, 2016; Conway, 2012).

In this sense, the successes of the new media technologies have been built on their democratic nature, by the propensity of their entrepreneurs to place them, to an extent, beyond the reach and control of states. This, however, means that, while the corporates are

[10] With the military successes of the US invasion of Afghanistan, and subsequently Iraq, the paradigm shifted further with the emergence and growing popularity of increasingly sophisticated Web 2.0 platforms, namely file-sharing portals and social networking sites (Conway, 2012). Here, al-Qaeda and its affiliates (such as *al-Qaeda in Iraq* (AQI)) began utilizing new developments in online media to disseminate downloadable content such as magazines, video and brochures.

[11] As a veteran of the Soviet–Afghan War, Al Zarqawi sought to legitimize himself in the eyes of the al-Qaeda leaders who did not wish to recognize his affiliation and role as the "manager of [al-Qaeda's]Iraqi franchise", as Maggioni (2015; 56) observes.

able to skim off the pay from this success, the harms of online violence are externalized to the victims (both user and non-user). Zizek has noted this ambiguity of 'online communism' when he observes that

> The very nature of the world wide web seems to be communist, tending towards the free flow of data- CDs and DVDs are gradually disappearing millions of people simply downloading music and videos, mostly for free…This free circulation, of course, brings its own dangers…this very openness gives birth to non-creative providers (Facebook, Google) who exert an almost monopoly power to regulate the flow of data, while individuals who create the content are lost in the anonymity of the network (2014: 54)

DIY Jihad

One of the results of the anonymity Zizek alludes to has been the emergence of the phenomenon others (such as Michael, 2013, and Veilleux-lepage, 2016) refer to as DIY Jihad. The purpose of DIY Jihad is to decentralize killing decision-making so that, on cue, umbrella outfits such as AQ and IS can reach their targets far and wide. Under DIY Jihad, the responsibility for carrying out attacks has been externalized to individual Jihadis who assumed entrepreneurial decision-making. This strategy has been most pronounced in the methodology of the *Al-Qaeda in the Arabian Peninsula* (AQAP): In 2010, AQAP launched a widely distributed English-language online magazine titled *Inspire,* which encouraged individual jihad against Americans and Westerners (Michael, 2013). *Inspire* combines sleek ideological material packed with simple instructions aimed, as it claims, at 'skill-building' for the ultimate aim of bringing to fruition the so-called caliphate (see also, Veilleux-lepage, 2016; Conway, 2012). In this sense, *Inspire* is the paradigm shift proper; it not only represents the proliferating 'skills-building' of radical Islam, but is also more effective at articulating the terms of violent jihad to English-speaking readers, by packaging it in terms familiar to their experiences.

Michael (2013) and Veilleux-lepage (2016) correctly point out that electronic jihad is the most potent tool because of its power to assuage the cognitive dissonance of individuals who wish to advance the jihadist cause but are unable or unwilling to partake in actual conflict. As an example, through a section entitled *Open Source Jihad*, *Inspire* provided details of how to conduct a random shooting in a crowded restaurant or how to weld

blades to the front of a pickup truck to 'mow down the enemies of Allah' (as quoted in Michael, 2013; 55). Actually, since *Inspire* there have been a number of high-profile attacks on western targets, including the attempted decapitation of the marine drummer Lee Rigby in London in 2013, and the attempted bombing of *Delta Airlines* by the 'underwear bomber' *Abdulmutallab*[12] (Kailemia, 2016). These and similar attacks were inspired by the strategic vision of *Anwar al-Awlaki*, a popular American-born cleric affiliated with AQAP, whose sermons were widely distributed on YouTube[13]. As Hoffman, (2010) has observed, this ability of terrorist organizations to motivate and empower individuals to commit acts outside of any chain of command, only using online material, represents a change in the nature of terrorism itself.

What Hoffman is already aware of is the fact that, for organizations such as AQ, the battle is not just for their so-called caliphate, but also for the online market share: That is, in order to achieve the social objective (of segregating their admirers), organizations such as IS and AQ increasingly rely on the dissemination of their message uniquely effective social media strategy[14]. Organizations such as IS have developed and relied on a range of exceptionally professional and sophisticated communication and social media initiatives that are exceptionally easy to access and highly attractive to their audiences, including publishing ebooks and eMagazines and professionally edited videos[15]. This extensive reliance on unaffiliated sympathizers (who either re-tweet or re-post content produced and authorized

---

[12] See http://www.independent.co.uk/news/world/americas/underwear-bomber-umar-farouk-abdulmutallab-begins-life-term-7018630.html

[13] According to Veilleux-lepage, (2006), al-Awlaki and *Inspire* led to a fundamental shift in al-Qaeda's strategy from organizationally-led jihad towards do-it-yourself terrorism. Similarly, Jarret Brachman (2014) claims that al-Awlaki and AQAP made do-it-yourself terrorism and its participants, the focus of their media efforts, rather than conceptualizing al-Qaeda's sympathizers as merely an audience.

[14] IS' *Dabiq*, for example, targets readers who are already interested in political Islam, but not necessarily already convinced jihadists. It attempts to 'educate' the reader on the caliphate's aims, projects, and accomplishments. Similarly, IS' "Black Flags Books,"- widely advertised on social media and jihadist forums- often uses infographics taken from Western media but presented from the caliphate's perspective (see also, Lombardi, 2015). Such texts systematically organize information and are thus an effective propaganda tool which is easily accessible to those who seek out information about the so-called caliphate.

[15] On 5 July 2014, as an example, IS media group *al-Hayat* released in numerous different languages (including Albanian, English, French, and German) the first issue of its online magazine *Dabiq*, a publication reminiscent of AQAP's *Inspire* magazine. With its slick and sophisticated production value, *Dabiq* defines itself as*"a periodical magazine focusing on the issues of unity (tawhid), truth-seeking (mamhaj), migration(hijrah), holy war (jihad) and community (jama'ah). It also contains photo reports, current events, and informative articles on matters relating to the Islamic State" (as quoted in Maggioni, 2015; 71).*

by IS leadership) has significantly driven up the usage of such media tools (Veilleux-lepage, 2016, Michael, 2013). As an example, when *Abu Bakr al-Baghdadi* declared the establishment of the IS 'caliphate', the message was uploaded on YouTube videos (and on the file-sharing website *justpaste.it*) before it was tweeted and re-tweeted millions of times by sympathisers (Veilleux-lepage, 2016). In similar vein 'hashtag hijacking,'- which involves the manipulation of popular twitter 'hashtags' as a means of infiltrating conversations- has been deployed by repeatedly, most prominently during the Scottish referendum elections when IS (Using the Twitter handle al-Furqan) advised its sympathisers to retweet the video showing kidnapped British photojournalist John Cantlin using the hashtag #Scotlandindependence (Vitale and Keagle, 2014).

The effectives and uniqueness of such media is, to make an obvious but no less important point, built on the backs of the externalized harms which individual victims and society collectively must bear. Such strategies, aimed at gaining maximum exposure and overcoming the censorship of media such as YouTube, nonetheless benefit such media by driving up the traffic on their sites (even if this is not originally intended)[16]. The problem with this, as Zizek (2009) and Chomsky (2015) warn us, is that it normalises 'symbolic violence': The democratization of online media, while purely a good thing, also brings with it its 'dark side'

Let us take another example.

D-I-Y (Revenge) porn and the victim 'entrepreneur-of-the-self'

As Linkous (2013:3) has observed, the proliferation of new technologies (and particularly the 'smartphone') has made it easy and more appealing for people to create and distribute Do-It-Yourself Pornography'. In the last two decades a major problem has emerged involving unauthorised distribution of nude images, mostly as a form of revenge (Stroud, 2014). Revenge Porn as a practice can have 'detriment effects' on the victim's lives[17]. As

[16] In another example, a clip of IS' film *Flames of War, posted* 18,034 views within just a seven-hour timeframe.

[17] The United Kingdom (UK) government has tackled the issue of Revenge Porn and in the *Criminal Justice and Court Act* (2015) which has a section specifically aimed at the crime of disclosing private sexual photographs with intent to cause distress. This works in tandem with EU law facility of the "right to be forgotten", which allows a person to request 'search engines to remove links with personal or damaging information about them'. However, as Bates (2015) notes, removal of search-engine link only makes the content harder to find, and does not necessarily mean that it has been deleted.

Franklin (2014: 1304) has noted, many of those who have fallen victim to revenge pornography have found themselves out of work, or forced to make major changes to their lifestyle, with victims even committing suicide. This is more so where, in addition to certain new media forums posting the pictures of victims, some (websites, for example) even offer visitors the facility of submitting their commentary on the images. Bates (2015: 63) shows how, in his study, 'many participants experienced more severe and disruptive mental health effects, often being given official medical diagnosis of PTSD'. Bates also shows how, in majority of the cases victims have a 'general loss of trust in people after being victimised by revenge porn, with many going from being very trusting to rarely trusting anyone' (2015: 61)[18]. Citron and Franks (2014: 348) have observed, apropos of 'revenge porn[19]', how we should 'no more blame individuals for trusting loved ones with intimate images than we blame someone for trusting a financial advisor not to share sensitive information on the street'. And yet the harms of revenge porn have been outsourced to the individual who, on top of falling victim to the crime, is also expected to take the blame and shame for not adequately preventing her own victimization.

Revenge Porn, and its related version 'sexting[20]', are perhaps the clearest index of the externalization of the capitalist harm to the individual. 'Victim-blaming', which Bates (2015: 18) defines as 'the act of unfairly accusing victims of contributing to their own victimization' is the norm in revenge porn. As Bates argues, victim-blaming can happen in many ways, including subtle questions 'asking a sexual harassment victim what they were wearing when they were sexually harassed, implying that if they had been dressed more modestly they would not have been harassed' (2015:18. The standard response to 'revenge porn' includes the disparaging of victims as "stupid" or "slutty" (Bates, 2015; Linkous, 2013). In one case where a Revenge Porn victim went to the police to get help the victim was told she 'shouldn't have taken the photo' (Bates, 2015). This is reflected in many other

[18] Altogether, wide research has that 'cyber harassment victims' anxiety grows more severe over time'; among younger victims of revenge porn victim have shown 'lower levels of academic performance, lower family relationship quality, a number of psychosocial difficulties, and affective disorders'.

[19]Revenge Porn has no clear definition because, as Bates (2015) explains, it may refer to all manner of non-consensual pornography (including images captured without a victim's knowledge, images of a victim's face transposed on a sexually explicit body, or hacked images, or images uploaded by jaded ex-lovers'.

[20] This encompasses a range of practices which include the exchanging of 'nude, semi-nude, or sexually suggestive images and text… via phones or on social network sites' (Linkous, 2013).

victims' reports about how they are dealt with many are told that 'if they did not want their nude photos to end up online, they should not have taken them in the first place' (Bates, 2015: 18).

The point not to be missed here is how apropos of revenge porn, little focus is placed in critical discourse on the role of online image security and how breaches of insecurity work in the reverse way; instead of damaging commerce (as would happen when corporations are hacked and data stolen, for example) revenge porn has a tendency to drive up the demand for the host so that, in a cynical twist, the gesture of breech serves the interests of the domain more.

Let us, lastly, render further the dichotomy between *'Meum and toom'* apropos of the externalized harms of cybercrime, through online school shooter fandoms.

School shooters and online fandom

A marked feature of postmodernity, Busse and Hellekson (2006:14) argue, is the emergence of online cultures over a shared appreciation or interest in a topic, with this shared interested specifically bringing together 'fans'. As we also saw apropos of online Jihad above, the rapid commercialisation of the internet in the late 1990s made people realise that engaging with the Web was going to be a vital part of modern living. The launch of "Web 2.0" democratized the internet, ushering not only the individual as an self-entrepreneur who could create and share their narrative with 'followers', but also fan clubs and fandom cultures which had hitherto interacted through radio and magazines (Nayar, 2010).

As Nayar argues, fandoms are a community of people built around a collective appreciation of "a star". In this sense, joining a fandom constitutes a form of 'space recovery' from social and also economic isolation[21]. It may also, as Duffet (2013) has argued, evidence an avenue for self-isolation. As Duffet argues, the fluidity of modern identity-making engenders a

[21] Some (for example, Bates, 2015) have actually claimed, the so-called 'information society', has weakened a sense of personal identity as society is bombarded by the media with suggestions of how we should be successfully living our lives in an acceptable manner e.g. through the right fashion, with a flawless face of make up or by aiming to replicate rich celebrity life styles. In other words, modern identity is based around consumable life-styles that people can pick and choose from to create themselves.

certain uncertainty so that online fandoms may be read as a form of escape from the plasticity of it all: Online fandoms may be a coping mechanism against the onslaught of 21st century consumerism. As such, those who struggle to find meaning (and voice) in the meaninglessness of post-politics bio-politics are externalized online (as the ranks of the depressed, distressed and so on) where they are preyed on even further, but away from the protective ambit of society (see also, Zizek, 2014). Those whom the imagery and symbolism of postmodernity isolates, Zizek argues, regain their camaraderie and reinforce identity online, even if fandom is the avenue to this end. The power of fandoms is thus that it provides the marginalized with new social codes and languages[22] (Baym 1998) which are necessary for their new 'virtual self' (Zizek, 2009).

But, the problem with the 'virtual self', the cyber-identity which is recreated, is that it can be completely different from real life identity: While the anonymity of the internet can be a good thing- for example where it allows suppressed identity (such as that of gay people) to be reasserted- it can also be a bad thing, especially when it provides a veil to conditions such as mental illness, anorexia or depression (or, in worse case scenarios, suicidal or terrorist drive) (Zizek, 2009; Bates, 2015). There isn't a clearer example of this than school shooter fandoms. The thread that unifies online school shooter fandoms is their shared obsession with violent, online content: Pekka-Eric Auvinen (the 18-year-old 'YouTube killer' who murdered 7 pupils and the principal of Jokela High School in Finland before later committing suicide) had, prior to his crimes, posted a wide range of videos on YouTube, in which he sympathised with school shooters, 'particularly those with a Nazi tinge" (Serazio 2010:428). Actually, just a few hours before his attack he even uploaded a video- entitled *'Jokela High School Massacre—11/7/2007'* - where he described his plans to kill later that day.

School shooters are thus another good example of the externalized harms of post-politics bio-politics: Where neo-liberal policies have succeeded in constructing the individual as an

[22]Zizek (2014) notes the existence of 'resistance identities' as 'generated by those actors who are in positions/conditions devalued and/or stigmatised by the logic of domination, thus building trenches of resistance and survival based on the basis of principles different from, or opposed to, those permeating the institutions of society"

entrepreneur-of-the-self to be rewarded, or shamed, concomitant to his participation in the circus of financialised consumerism (Lazzarato, 2011; Zizek, 2014), sometimes the 'chickens come home to roost' in the shape those who rebel (albeit out of delusion) against this logic, with disastrous consequences. As Rico (2015) has shown, the columbine shooters, Klebold and Harris, claimed that they were resisting the subordination of "moronic" mainstream society which they rejected and looked down upon. Equally, fandoms which have developed in the wake of Columbine shooting often justify the heroics of Klebold and Harris by contrasting it to the pressures of a 'rigged' educational, economic or political system.

Conclusion

In conclusion, the frame of analysis deployed above is not new or unique: Criminologists and critical theorists have lately tended to engage with the 'harms' of capital (Lazzarato, 2011; Kovel, 2007; Foster, et al. 2010), with growing literature highlighting, in particular, the 'externalized' harms of corporations (Stiglitz, 2012; South, 2013; Ruggierro, 2013; Klein, 2002). Such critique has singled out the issues of power inherent in access, exploitation and commercialisation of common resources, and how this constitutes, for those who lack such power, a form of subjectivation (Lazzarato, 2011; Zizek, 2014). This subjectivation has also been related to contemporary externalization of harms through transnationalization (under what is commonly known as 'globalization') (Stiglitz, 2012; Gros, 2003; Aas, 2007). The conclusion drawn is that the harms of postmodern capitalism (and specifically, neoliberalism) are borne, not just by the biological system as a whole (in terms of species loss, displacement and so on) but also by the multiplier-effect on health and safety (from conflicts and displacement over natural resources, corruption and loss of revenue, deaths from mudslides or diseases, from cancers, mental illness and so forth) (Ruggiero, 2013; Ruggiero and South, 2013)

The main achievement of this paper has been to render the problems of (certain types of) cybercrime from a fresh analysis which is not boggled in 'techno-speak'; that is, we have engaged with the sociological problems of cybercrime, demystifying it as a technical challenge which should be separated from its proper roots in the political economy. The main achievement is in rendering not just the isolating nature of communication

technology, but also how this isolation both breeds violence and is itself a form of violence. This is important because we have stepped aside from the usual obsession with subjective violence (of bombs and knives and guns) to show the systemic roots of this violence (in the structure of the economy and language) (Chomsky, 2014; Zizek, 2009), at least as far as online interaction is concerned.

Of course space does not allow us to canvass all the points in relation to the political economy of technology, nor the harms of capital. We hope, nonetheless, that the small steps taken above will make vivid to the reader the extent and depth of online 'ecological disorganization', which Lynch et al. (2013:1) define as 'the ways in which human preferences for organizing economic production consistent with the objectives of capitalism are an inherent contradiction with the health of the ecological system'.

Bibliography

Aas, K. F. (2007) 'Analysing a World in Motion: Global Flows Meet Criminology of the Other' *Theoretical Criminology* 11 (2) 283-304

Agnew, R (2010) A general strain theory of terrorism, *Theoretical Criminology* 14: 131152Awan, A. N. and Al-Lami. M. (2009) Al-Qa'ida's Virtual Crisis, *The RUSI Journal,* 154(1), 56-64.

Bande, L. C. (2013) The Making of Cybercrime Legislation in Malawi: A Comparative Analysis of Malawi's Proposed Cybercrime Law against International Standards. Ph.D. *Katholieke Universiteit Leuven*

Bates, S. L. (2015) "Stripped": an analysis of revenge porn victims' lives after victimization (Doctoral dissertation, Arts & Social Sciences: School of Criminology, Keele University).

Baym, N. (1998) The Emergence of Online Community. In: S. Jones, ed., *Cybersociety 2.0*: *Revisiting Computer-Mediated Community and Technology*, 1st ed. SAGE Publications.

Brenner, S. W. (2007) Cybercrime: re-thinking crime control strategies. In: Y. Jewkes, ed. 2007. Crime Online, Devon: Willian Publication. pp.12-28.

Calvert, C. (2013) Revenge porn and freedom of expression: Legislative pushback to an online weapon of emotional and reputational destruction, *Fordham Intellectual Property, Media and law journal*, 24: 673.

Castro, T. and Osório, A. (2012) Online violence: Not beautiful enough... not thin enough. Anorectic testimonials in the web, *Psychology Journal*, 10(3)

Chomsky, N (2014) *How the world works*, New York: Penguin.

Citron, D. K., & Franks, M. A. (2014)Criminalizing revenge porn, *Wake Forest Law Review, 49: 345.*

Coleman, E. (2012) Phreaks, Hackers, and Trolls. In: M. Mandiberg (ed.) *The Social Media Reader*, 1st ed. New York and London: New York University Press.

Conway, M. (2012) From al-Zarqawi to al-Awlaki: The emergence and development of an online radical milieu. *CTX: Combating Terrorism Exchange*, 2(4):12-22.

Cottee, S (2010) Mind Slaughter: The Neutralizations of Jihadi Salafism, *Studies in Conflict and Terrorism* 33 (4): 330- 352

Cullen, D. (2015) Interviewed by Brent Bambury on 'inside the online subculture of Columbiners'. CBC Radio, 21st February 2015

Curran, J. (2012) in Curran, J., Fenton, N. and Freedman, D. (2012) *Misunderstanding the Internet,* London: Routledge.

Daggett, C. (2015). Eric Harris and Dylan Klebold: Antiheroes for outcasts. Journal of Audience and Reception Studies, 12(2), pp.45-77.

Diamond, A. (2012) Anyone can fall foul of a scam – and I'm proof of that. Which?, [online] Available at: https://conversation.which.co.uk/money/bank-scams-natwest-phishing/

Dietz, P. E. (1986) Mass, serial and sensational homicides. *Bulletin of the New York Academy of Medicine*, 62(5): 477–491.

Dobson, A. S., & Ringrose, J. (2016) Sext education: pedagogies of sex, gender and shame in the schoolyards of Tagged and Exposed. *Sex Education,* 16(1): 8-21.

Duffet, M. (2013) *Understanding Fandom: An Introduction to the Study of Media Fan Culture*, USA: Bloomsbury Publishing.

Fieldland, E. (2014) The Islamic State (ISIS) Fact Sheet. Clarion Project. Retrieved from www.clarionproject.org/factsheet/islamic-state-isis-isil.

Franklin, Z. (2014) Justice for Revenge Porn Victims: Legal Theories to Overcome Claims of Civil Immunity by Operators of Revenge Porn Websites. *California Law Review*, 102:1303.

Goforth, P. (2016) The Characteristics and Typologies of School Violence Perpetrators. In: G. Crews, ed., *Critical Examinations of School Violence and Disturbance in K-12 Education*, 1st ed. IGI Global, pp.85-96.

Gros, J., G. (2003) 'Trouble in Paradise: Crime and Collapsed States in the Age of Globalisation' *British Journal of Criminology* 43 (1): 63-80

Hayek F (1973) *Law, Legislation and Liberty*, London: Routledge & Kegan Paul.

Hellekson, K. and Busse, K. (2006) *Fan fiction and fan communities in the age of the Internet*, Jefferson, N.C: McFarland & Co.

Hoeren T. & Vossen, G. Manifest: The Role of Law in an Electronic World Dominated by Web 2.0. *Computer Science Research and Development,* 23(1), 7-13.

Hoffman, B. (2010, July 21).The American Jihad, Part II. The National Interest. Retrieved from http://nationalinterest.org/commentary/american-jihad-part-ii-3680.

Johnson, B., 2008. Nurse handed over $400,000 to web scam despite FBI warning. The Guardian, [Online] 15 November. Available at: http://www.theguardian.com/technology/2008/nov/15/internet-usa

Kailemia, M (2016) International Justice in the time of 'outsourced illiberalism'; Africa and the International Criminal Court, *Journal of Global Faultlines* (3): 16-28.

Kalish, R. and Kimmel, M. (2010) Suicide by mass murder: Masculinity, aggrieved entitlement, and rampage school shootings, *Health Sociology Review*, 19(4): 451-464.

Kiilakoski, T. and Oksanen, A. (2011) Cultural and peer influences on homicidal violence: A Finnish perspective, *New Directions for Youth Development*, 2011(129): 31-42.

Klein, N (2002) *No Logo,* New York: Picador.

Laird, L. (2013) Striking Back at Revenge Porn: Victims Are Taking on Websites for Posting Photos They Didn't Consent To. *ABA Journal*, 99:45.

Lazzarato, M (2011) *The making of the Indebted man*, Semiotext(e)

Lazzarato, M (2014) *Signs and Machines; Capitalism and the production of Subjectivity*, Semiotext(e)

Kowalski, R. M., Limber, S. P., and Agatston, P. W. (2012) Cyberbullying: Bullying in the digital age. John Wiley & Sons.

Linkous, T. (2013) It's Time for Revenge Porn to Get a Taste of Its Own Medicine: An Argument for the Federal Criminalization of Revenge Porn, *Richmond Journal of Law and technology* 20:1.

Maggioni, M. (2015), The Islamic State: Not That Surprising, If You Know Where to Look, In Twitter and Jihad: the Communication Strategy of ISIS, edited by Monica Maggioni and Paolo Magri, *Italian Institute for International Political Studies*, 49-81.

Michael, G. (2013) The New Media and the Rise of Exhortatory Terrorism, *Strategic Studies Quarterly Spring*, 7(1), 40-68.

Moyo, D (2009) Dead Aid; Why aid is not working and how there is another way for Africa, Allen Lane, London.

Nayar, P. (2010) An introduction to new media and cybercultures, Chichester, West Sussex, U.K.: Wiley-Blackwell.

Pfeifer, B. and Ganzevoort, R. (2015) The Implicit Religion of School Shootings, *Journal of Religion and Violence*, 2(3), pp.447-459.

Rico, A. (2015) *Transformative Works and Cultures*, (19).

Rocque, M. (2012) Exploring school rampage shootings: Research, theory, and policy. *The Social Science Journal*, 49(3): 304-313.

Ruggiero V (2013) *The Crimes of the Economy*, London: Routledge.

Ruggiero V and South N (2013) *Green Criminology and crimes of the economy: Theory, research and praxis*, Critical Criminology.

Schnaiberg, A. (1980) *The Environment: From Surplus to Scarcity*, Oxford University Press.

Serazio, M. (2010) Shooting for Fame: Spectacular Youth, Web 2.0 Dystopia, and the Celebrity Anarchy of Generation Mash-Up, *Communication, Culture & Critique*, 3(3):416-434.

Stiglitz J (2012) *The Price of Inequality*, London: Allen Lane.

Stroud, S. R. (2014) The dark side of the online self: A pragmatist critique of the growing plague of revenge porn, *Journal of Mass Media Ethics*, 29(3):168-183.

Talbot, D. (2014, February 1). Terror's Server. Technology Review. Retrieved from http://www.technologyreview.com/featuredstory/403657/terrors-server/.

Quarshie, H. O. and Odoom, A. (2012) Fighting cybercrime in Africa, Scientific & Academic Publishing, [online] Available at: http://article.sapub.org/10.5923.j.computer.20120206.03.html#Ref

Vitale, H. M., & Keagle, J.M. (2014) A Time to Tweet, as well as a Time to Kill: ISIS' Project of Power in Iraq and Syria. Institute for National Strategic Studies. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/defensehorizon/DH-77.pdf

Wall, D. S. (2007) Cybercrime. Cambridge: Polity Press.

Weimann, G. (2006) Terror on the Internet: The New Arena, the New Challenges. *Washington, DC: United States Institute of Peace.*

Yar, M. (2013) Cybercrime and Society, 2nd ed., London: SAGE Publication Limited.

Zizek, Slavoj (2009) *Violence*, Profile Books: London.

Zizek, Slavoj (2010) *The Year of dreaming dangerously*, Verso Books: New York.

Zizek, Slavoj (2014) *Trouble in paradise; from the end of history to the end of capitalism*, Penguin, New York.